



January 28, 2011

The Honorable Gary Locke  
Secretary of Commerce  
U.S. Department of Commerce  
National Telecommunications and Information Administration  
1401 Constitution Ave., N.W., Room 4725  
Washington, D.C. 20230

RE: Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework, RIN 0660-XA22

Dear Secretary Locke:

We are pleased to submit these comments on the Green Paper on behalf of The Future of Privacy Forum (FPF), a Washington, DC based think tank that seeks to advance privacy through responsible data practices. The forum is led by information privacy experts Jules Polonetsky and Christopher Wolf and include an advisory board comprised of leading figures from industry, academia, law and advocacy groups.<sup>1</sup>

At the outset, we commend the Department and its Internet Policy Task Force for its leadership and insights on improved consumer privacy reflected in the Green Paper. The Green Paper, as well as the currently pending FTC Staff Report on

---

<sup>1</sup> The views expressed herein are not necessarily those of the members of the Advisory Board or sponsors of The Future of Privacy Forum.

privacy, contribute enormously to the advancement of privacy in the United States. As noted in the Green Paper, privacy is an essential element of consumer trust, and is beneficial both to people and to business. As a result, privacy is important to the U.S. commerce and our economy.

We enthusiastically support the proposal for a Privacy Policy Office within the Department to work with industry sectors and the FTC to develop voluntary but enforceable codes of conduct. Indeed, the FPF called for a senior level Chief Privacy Officer as item number 1 on our Privacy Agenda for the New Administration,<sup>2</sup> and expressed our support for a Privacy Policy Office upon the announcement by Assistant Secretary of Commerce Larry Strickling that the Commerce Department would be calling for the creation of such an Office.<sup>3</sup>

Our comments below do not respond to every question raised in the Green Paper, but rather provide input in selected areas based on FPF's activities and experience in examining consumer privacy.

#### Question 2.

a. What is the best way of promoting transparency so as to promote informed choices?

The range of consumer types needs to be considered in determining how best to promote transparency and informed choice. There are some consumers who take their time to review carefully the details of a company's data use and to make informed choices; for these consumers, accessible privacy policies that provide details will be useful. Admittedly, this category of consumer is rare. And even within this category, there will be times when such normally careful consumers do take the time or effort to investigate data practices of every business with whom they deal. At the other end of the spectrum, and we believe more typical, are consumers who rarely expend the effort to examine the stated data practices of a business. Transparency and choice solutions need to be crafted to serve this range of audiences.

Just as web sites are designed to immediately inform a visitor of the purpose of the site and its features, in order to make a sale or attract viewers, there needs to be a mechanism to immediately inform consumers of how their data will be treated. In this way, the consumer type that more typical – the one that rarely digs deep to

---

<sup>2</sup> <http://www.futureofprivacy.org/2009/01/19/the-future-of-privacy-forum-consumer-privacy-agenda-for-the-new-administration>

<sup>3</sup> <http://www.futureofprivacy.org/2010/11/12/a-us-privacy-leader>



understand a business' data practices – will be informed in a simple, clear and immediate way.

Techniques to inform consumers of data practices might include symbols, short phrases, colors, diagrams, dashboards or any of the tools available to a designer who seeks to provide users with an engaging user experience. Engaging consumers about data use must be seen as an essential feature and a core part of the user experience. Once companies embrace this concept, innovators and creative designers can take on the challenge of simplifying the description of complex practices and providing appropriate choices.

We think the use of symbols and icons, such as the “forward I” adopted by the Digital Advertising Association is an important achievement in this area and FPF was pleased to conduct some of the original research around the use of icons for behavioral advertising communications. We are also pleased to see the way Apple’s iPhone uses an arrow to indicate in an immediate way that location sharing is occurring. We commend the development of privacy icons by Mozilla. We look forward to seeing studies evaluating the effectiveness of these techniques in informing consumers, and to the development of similar indicative tools in the future.

## Question 2

k. Do industry best practices concerning purpose specification and use limitation exist? If not, how could their development be encouraged.

Retention limits are critical use limitation. Quite simply, if data is not retained, it cannot be used.

The setting of limited retention periods by companies is relatively new for some. We welcome that development. For example, prominent ad networks and search engines have committed to specific retention periods and to the deletion of data after a period of time. Only a few years ago, it was extremely rare to find such a limitation expressed in a company privacy policy.

As recently as several years ago, ad networks kept logfile level data for indeterminate amounts of time. Today, many companies have settled on three, six or nine months as potential time frames for retention of log files used for behavioral advertising. Search engines have partially anonymized data at three, nine, or eighteen months and continue to react to the demand of the Article 29 Working Party in the EU that more limited retention must be implemented. Analytics

companies have been less transparent about data retention practices, but some have set thirteen months as their maximum reporting time.

A companies' need to retain data can change over time, due to competition, security and fraud detection concerns or other factors. The emerging privacy framework must allow flexibility for companies with respect to retention periods, but still should encourage limited retention as a benchmark. Thus, laws or regulations specifying retentions periods, and setting them in stone, is not advisable.

### Data Enhancement

Improved practices around data "enhancement" should focus on the practice of appending data used online to target ads across unrelated web sites. A significant portion of the data used today for ad targeting is data about consumers that has been appended to a cookie. Current industry standards are unclear as to when and how enhanced notice or choice applies to such data. Consumers who do not understand or who feel they have control over this process are likely to express the same concerns that they have about behavioral advertising based on web site visits or searches. The practice of appending offline data that was the subject of great controversy nearly a decade ago following the DoubleClick-Abacus merger are now commonplace, but standards for such data merger have not continued to evolve.

### Sensitive Information

No issue is more in need of consumer research than the issue of defining sensitive data. Of course there are clear areas where certain data has already been well defined as subject to special requirements, such as data covered by HIPPA, GLB, FCRA, etc. However, there is wide diversity in practices around the use of certain non-personal categories of data for online marketing. Ad networks owned by Yahoo, AOL and Microsoft generally maintain internal lists of restricted categories that will not be made available for sales purposes. But these lists are far from uniform, and are based on the editorial judgment of company executives. Some companies<sup>4</sup> refrain from using data about a consumer's visit to a health-related web sites, others do use health data but refrain from creating certain categories such as cancer or incontinence or Viagra. Other companies actively market health related profiles without reservations. Industry self-regulatory efforts currently limit or require affirmative consent for relatively narrow classes of data. The International Privacy

---

<sup>4</sup> DoubleClick does not use sensitive health data for behavioral ads, except for re-targeting visitors to a website by that same company.



Pharmaceutical Privacy Consortium has issued a number of white papers on privacy but has yet to take a position in this area.

Although research studies have looked at general consumer views of behavioral ads, very little work has been done in the area of understanding whether consumers differentiate between various types of health information used in this manner. The Department of Commerce should explore avenues at its disposal to encourage research into consumer sensitivities in this area.

## Question 2

n. How can purpose specifications and use limitations be changed to meet changing conditions?

Purpose specifications and use limitations are important but cannot be a straightjacket. Companies may need to use data in new or innovative ways. Consider, for example, the initial rollout of the Facebook Newsfeed. Early in its development, Facebook users would visit their own profile page when they signed in and would click to their Friends' pages to learn any new information that their friends had posted or any changes made to their Friends' profiles. Then Facebook launched the Newsfeed that began automatically sharing any changes made by a Facebook user to the pages of their Friends. Many users were surprised by this and a large portion of the user base joined Facebook Groups expressing opposition to this change. Certainly, few would have opted into this feature in a blanket manner. Despite the fact that this feature would likely not have been considered "Commonly Accepted" due to its novelty and the manner it used data, it soon became an essential part of the Facebook experience and was soon copied by competitors. Today, much of the Facebook user engagement is related to users interacting with the Newsfeed where they learn about their Friends' activities.

Contrast, however, the Facebook Beacon program, where users were alarmed and the program did not succeed. Beacon was a new Facebook feature which sent data from external websites to Facebook for the purpose of sharing users activities with their Friends. Certain activities on partner sites were published to a user's News Feed. How can a policy distinguish between these two examples? We propose the following framework:

If a new use is within the scope of the previously defined uses, no new consent would need to be obtained from users. If a new use is beyond the scope of the previously outlined uses, the company would then be required to complete a privacy impact assessment. Additionally, if the change involves: (a) sharing the

information with additional parties; (b) an added risk of harm to the user; (c) advertising or marketing-related data; (d) making a material change to the way data is handled; or (e) makes something public that was not previously, the change would require affirmative consent by the user. If the new use is transparent and obvious to users, and also provides added value to the user, an opt-out system would be permissible as long as the opt-out is clear and conspicuous.

We think such a framework would prevent harm, assure user autonomy, and allow room for the continued innovation in providing new and novel services for consumers.

#### Question 4.

b. How can the Commerce Department best encourage the discussion and development of technologies such as “Do Not Track”.

The amorphous concept but enticing terminology of Do Not Track (“DNT”) has dominated much of the public discussion about privacy in recent months. Unfortunately, in our view, much of this discussion has been unproductive, with some in industry suggesting that DNT would bring an end to ad-supported online content, and some privacy advocates viewing it as a silver bullet solution for perfecting online privacy. However, very little constructive dialogue has occurred across stakeholder groups. And browser companies, online businesses, and advocates have by and large formulated their views without collaboration.

In 2009, FPF, in cooperation with the Center for Democracy and Technology, launched an effort to improve the current cookie based opt-out mechanism offered by many online behavioral advertising companies.<sup>5</sup> Aware of the fact that many opt-out cookies are deleted by consumers or their anti-spyware programs, we convened companies, trade groups, advocates and technologists for a number of discussions aimed at formulating a more reliable process for providing consumers with options to limit the web tracking taking place for behavioral advertising purposes.

In 2010, FPF responded to the FTC’s DNT proposal, by convening a panel that included representatives from browser companies<sup>6</sup>, consumer and privacy organizations<sup>7</sup>, technologists, ad networks, and policy groups. Although no

---

<sup>5</sup> Many online analytics companies offer consumers a similar cookie based opt-out choice.

<sup>6</sup> Sid Stamm represented Mozilla on the panel and Internet Explorer product manager Dean Hachamovitch attended the program.

<sup>7</sup> Michelle DeMooy of Consumer action and Erica Newland of CDT presented.



consensus emerged, we were convinced that a properly tailored and practically designed DNT proposal was feasible. We describe this proposal in the following paragraphs.

#### Browser companies:

Browser companies should provide consumers with an option in the preferences panel of the browser that would enable a special HTTP header. In addition, browser companies should provide an API that web sites or services could use for the purpose of setting this header for consumers. Ensuring that parties other than the browser companies could activate this option for users would ensure that this option can be promoted by third parties, including government, advocates and trade groups. It would also ensure that the option would be compatible with the self-regulatory program already in place that has been adopted by many leading trade groups. The announcement made by Firefox that it would adopt an opt-out header is almost identical to what we propose here, other than the ability of web sites to set the header for users.

#### Ad Networks:

Servers that are sent this header should recognize that the consumer has indicated that they do not want their online activity used to tailor advertising to them across unrelated web sites.<sup>8</sup> Services that offer consumers a cookie based opt-out should therefore treat consumers presenting the header in the same manner they treat consumers relaying an opt-out cookie. Since opt-out cookies are often deleted inadvertently by consumers, this header will provide greater stability and a more reliable means of recognizing consumer choices.

For users who present the header, companies should also refrain from appending data to follow the users' activity across web sites. Companies should be required to recognize the header to indicate "no targeting" based on previous unrelated activity, whether tracked via cookies, device fingerprinting, local shared objects, or other identifiers. Such header should not affect tailoring of advertising for a user as the result of inferences made about a user based on the presentation of browser information or activity during a consumers' visit to a particular web site. Thus geo-targeting based on IP address or tailoring of ads based on a consumer's previous visit to the same web site should be permitted.

---

<sup>8</sup> We use the term "unrelated" here to mean from the perspective of the reasonable consumer.

### Consumers:

Consumers today can technically prevent tracking by using cookie settings or browser based options or third party browser plug-ins that limit the data that is shared by browsing activity. But the available options are unable to distinguish between the various types of uses of data by sites. These tools either underblock, overblock, or in some cases completely prevent, the delivery of third-party content or ads. Although the technology embodied in P3P in theory could provide greater level of distinguishing use, the manner in which it has been implemented in browsers and the distinctions between types of data use it provides often do not map easily to the prevalent business models in use. Many consumers who today take steps to block cookies are likely expressing their opposition to behavioral advertising. An opt-out/DNT header provides those consumers with a more nuanced opportunity to express their choice.

### Government:

We believe that the most productive way to advance a proposal such as the above is to convene a multi-stakeholder group that can work through the necessary cooperation between browser companies, ad networks, consumer representatives, government and policy groups. No system requiring nuanced cooperation and technology development across business models and government policy will spring into existence without interactions that can address the concerns of the key stakeholders. We suggest that the Department of Commerce partner with the FTC to convene such a group, in a process much as the Commerce has called for in its Report. We recognize that Internet Explorer and Chrome have generated alternative approaches and we appreciate the benefits of those approaches. Bridging the approaches of the different browsers would be well suited to a multi-stakeholder solution.

Another practical way the federal government could advance such a proposal would be to itself takes steps to respect the DNT header when users have selected this preference.<sup>9</sup>

---

<sup>9</sup> See proposal by technologist and DNT evangelist Chris Soghoian at <http://paranoia.dubfire.net/2011/01/what-us-government-can-do-to-encourage.html>



Question 9.

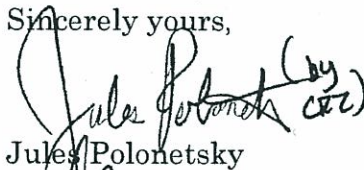
a. Should a pre-emption provision of national FIPS-based commercial data privacy policy be narrowly tailored to apply to specific practices or subject matters, leaving states free to regulate new concerns that arise from emerging technologies? Or should national policy, in the case of legislation, contain a broad pre-emption provision.

No market is more national than the online data market. Services that would need to meet many different state obligations would drastically increase costs and contribute to a poor user experience. With limited exceptions, rules for online data use should be national in scope.

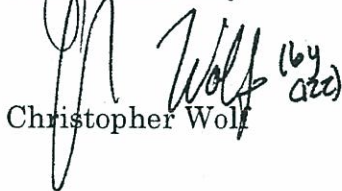
\*\*\*\*\*

We hope these comments contribute to the ongoing efforts of the Department to advance responsible and dynamic practices and we look forward to continuing to support the agencies leadership in this area.

Sincerely yours,

 (by  
Jules Polonetsky (cc)

Jules Polonetsky

 (by  
Christopher Wolf (cc)

Christopher Wolf